DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
2 NAVY ANNEX
WASHINGTON, DC 20380-1775

MCO 3432.1
PS
30 Jul 02

MARINE CORPS ORDER 3432

From: Commandant of the Marine Corps
To: Distribution List

Subj: THE MARINE CORPS OPERATIONS SECURITY (OPSEC) PROGRAM

Ref: (a) DOD Directive 5205.2, DOD Operations Security Program of 29 November 1999
(b) Joint Pub 3-54, Joint Doctrine for Operations Security of 24 January 1997

Encl: (1) Examples of OPSEC Indicators
(2) Examples of Critical Information
(3) Examples of OPSEC measures
(4) The OPSEC Process
(5) The OPSEC Survey
(6) Inspector General’s Checklist

1. Purpose. To establish policy, responsibilities, and procedures for the Marine Corps Operations Security (OPSEC) Program.

2. Scope. This Order applies to all Marine Corps activities, installations, commands, units, and personnel (to include personnel form other services and civilian employees serving with Marine Corps units). Marine Corps components that do not possess critical information and with no activities that could affect national security are exempt from this Order. Commanding Generals listed in paragraph 6 b and c of this Order are the approving authorities for OPSEC program exemptions.

3. Definitions. The following terms and concepts must be understood for successful OPSEC:

a. OPSEC Indicator. These are friendly detectable actions and open sources of information that adversary intelligence systems can potentially detect or obtain and then interpret to derive friendly critical information. Enclosure (1) lists examples of OPSEC indicators.

b. Critical Information. These are specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. Enclosure (2) lists examples of critical information.

c. OPSEC Vulnerability. This is a condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide for a basis for effective adversary decision-making.

d. OPSEC Measures. These are actions taken to reduce the probability of an enemy from either collecting OPSEC indicators or to

DISTRIBUTION STATEMENT A: Approved for public release, distribution is unlimited.

correctly analyze their meaning. Enclosure (3) provides examples of OPSEC measures.

4. General. Information Operations (IO) are actions taken to influence, affect or defend information, information systems and decision-making. The objective of IO is to influence adversary decision-making while protecting friendly decision-making. OPSEC is one of the core IO capabilities that also include Psychological Operations, Military Deception, Computer Network Operations, and Electronic Warfare. Supporting these core IO functions are Counterintelligence, Physical Security, Information Assurance, and physical attack. All of these activities must be supported by timely and accurate intelligence.

a. OPSEC is an operations function, not a security or an intelligence function. Security functions prevent unauthorized access to personnel, equipment, facilities, materials, and documents. Intelligence activities provide information on adversary forces, governments, and intentions. Counterintelligence identifies adversary intelligence assets, processes, and activities. OPSEC and these activities often overlap and are mutually supportive. Close coordination must be maintained between all staff functions to ensure adequate OPSEC protection. OPSEC is just one aspect of the overall effort for mission success, but it is one that every Marine can materially affect on a daily basis. Remember, OPSEC, like camouflage, is a continuous process.

b. OPSEC is a process of identifying critical information and then analyzing friendly actions concerning military operations and other activities to:

(1) Identify those actions that can be observed by adversary intelligence systems.

(2) Determine what OPSEC indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

(3) Select and execute OPSEC measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

5. Policy

a. Requirements. Reference (a) requires the Marine Corps to establish an OPSEC program. Reference (b) is an excellent source for information on planning and executing OPSEC programs.

b. Purpose. Protection of critical information must become an integral part of our daily operations and training. The ultimate purpose of OPSEC is to prevent an adversary or potential adversary from obtaining critical information that facilitates the prediction of friendly intentions, capabilities, and activities. Compromise of critical information can allow the enemy to “shape the battlefield.” Denial of critical information to the enemy will contribute to the “fog of war” and can result in flawed command decisions that hinder the enemy’s efforts while enhancing our operations.

c. OPSEC is a Command Responsibility. The operations staff (S-3/G-3) is responsible for assisting the commander in planning and execution of the command's OPSEC program. Close coordination with members of the commander's staff, attached and supporting elements, and any joint and/or coalition forces involved are vital.

d. OPSEC Process. Commanders shall apply the OPSEC Process as detailed in enclosure (4). OPSEC is a five-step process that entails:

(1) Identification of critical information

(2) Analysis of threats

(3) Analysis of the vulnerabilities

(4) Assessment of risks

(5) Application of OPSEC measures

e. OPSEC Survey. The OPSEC survey is an intensive application of the OPSEC process to an existing operation or activity by a multi-disciplined team of experts. Enclosure (5) details the OPSEC survey. Commanders should tailor the survey to their specific requirements. To begin the survey, critical information must be identified. Without critical information, a determination that vulnerabilities exist cannot happen. The OPSEC survey determines if the critical information is being protected. OPSEC surveys evaluate the OPSEC measures and if needed, recommend changes to existing measures. The survey can also identify requirements for additional OPSEC measures.

f. Threats. We must take into account the various threats to our Marine Corps and other DOD components in joint operations, especially in light of recent terrorist attacks and current threats. We must safeguard our critical information from traditional enemy intelligence forces and non-conventional forces. The enemy we face today may not wear a uniform and be part of a national force already in our intelligence database. Marines in all stages of activities (e.g., garrison and field operations), anywhere in the world, are potential targets. With the advanced technology and tempo of media operations, information available on the Internet, and freedom of movement within the United States, there exists a greater opportunity for our enemies to collect intelligence. Enemies can collect information through these open sources. This information is usually not protected and open to the public. Information collected over a period of time, often over a period of years, can paint a picture our vulnerabilities. Commanders must be aware of this and practice OPSEC not just in war, but also at all times.

g. Excessive OPSEC. Excessive OPSEC can degrade operational effectiveness by interfering with activities such as coordination, training, and logistical support. Military operations are inherently risky, and the commander must evaluate each activity and operation, and balance required OPSEC measures against operational needs. Using the OPSEC process will help commanders assess the risk and apply the appropriate OPSEC measures.

h. Public Affairs. Public affairs are important to garner public support and foster community relations to help with success of military operations. Because of advanced technology, instant media coverage and public knowledge of military operations is inevitable. Public affairs staffs must be included in the OPSEC planning process where media attention is expected and is desired. The need for OPSEC should not be used as an excuse to deny noncritical information to the public.

i. Importance. The old adage, ”loose lips sink ships” is still relevant but is not enough to protect critical information. A relevant OPSEC program will help to ensure OPSEC success. Marines and civilian employees are the most critical elements for successful OPSEC. Commanders must ensure that their personnel incorporate OPSEC fundamentals into their daily routine. Unit OPSEC programs shall provide for formal training to educate personnel on OPSEC procedures and to raise awareness. Commanders and other leaders will continuously practice OPSEC and stress the importance of OPSEC to mission success.

6. Tasks

a. Director, Security Division (PS), PP&O, HQMC:

(1) Develop and maintain an OPSEC order for the Marine Corps.

(2) Serve as the lead office on OPSEC matters for the Marine Corps.

(3) As required, coordinate OPSEC matters with other DOD agencies.

b. Commanding Generals, Marine Forces Pacific, Marine Forces Atlantic, Marine Forces Reserve:

(1) Develop and maintain a force OPSEC order.

(2) Designate those commands, units, activities, and installations under your cognizance that require an OPSEC program. You are authorized to delegate this authority down to the commanding generals, Division/Wing/Force Service Support Group, or equivalent activity and installation commanders.

c. Commanding Generals Marine Corps Combat Development Command, Marine Corps Recruiting Command, and Marine Corps Material Command:

(1) Develop and maintain an OPSEC order.

(2) Designate those bases, installations, and activities under your cognizance that require an OPSEC program.

d. Commanders: If required, establish an OPSEC program in accordance with this Order. The program, at a minimum, shall include:

(1) Designation of subordinate units or activities requiring an OPSEC program. This will eliminate the burden imposed by applying OPSEC to operations and activities that do not possess critical information and entail minimal risk to national security.

(2) Assignment of responsibility for your command and subordinate commands' OPSEC programs development, implementation, and oversight.

(3) Published commander's guidance and standard operating procedures (SOPs) to conduct a baseline OPSEC survey for the unit. The survey shall be reviewed and updated annually.

(4) Guidance and SOP for OPSEC surveys to evaluate the OPSEC process for operations and activities to be conducted as directed by the commander. This may be the same as the SOP for the baseline survey or be modified and tailored at the discretion of the Commander.

(5) SOP for the OPSEC process to be conducted and included in unit operational plans.

(6) SOP for an annual review and update of the command OPSEC program.

(7) Annual OPSEC education and awareness training for all personnel.

(8) Application of the OPSEC process to commands involved in acquisition, contracting, testing, and evaluation of weapons and systems possessing critical information where disclosure poses a risk to national security. This OPSEC requirement is in addition to other applicable directives.

e. Director Command, Control, Communications, Computers (C4):

(1) Continuously monitor USMC websites through the Marine Web Risk Assessment Cell program.

(2) Assist Marine Forces in ensuring that the appropriate safeguards are in effect for information posted to a website.

(3) Direct the removal of information from websites that violate OPSEC standards unless adequate safeguards are employed.

E. R. BEDARD
Deputy Commandant
Plans, Policies, and Operations

DISTRIBUTION: PCN 10203296000

Copy to: 8145001 (1)

OPSEC INDICATORS

1. There are five basic characteristics to an OPSEC indicator that make them potentially useful for deriving critical information. The following characteristics must be understood to develop effective OPSEC measures.

a. Signature. A signature is the characteristic of an indicator that makes it identifiable or causes it to stand out. An indicator's uniqueness reduces the ambiguity of the indicator and minimizes the number of other indicators that must be observed to confirm a single indicator’s significance or meaning. For example, a thermal-imaging satellite detects an infrared heat exhaust emission at an expeditionary field. Analysis of the emissions indicates it is a ground equipment unit used for medium or large fixed-wing transport aircraft. The enemy analysts had previously identified different emissions from ground support equipment (GSE) and identified them as belonging to a particular aircraft or types of aircraft. The analyst only needs to look into their database to compare this recent indicator to identify what type or class of aircraft the GSE is being used for.

(1) An indicator’s signature stability implies constant or stereotyped behavior that allows an enemy to anticipate future actions. Reducing the uniqueness or stability of the indicator’s signature increases the ambiguity of the enemy’s observations.

(2) Procedural features are important to a signature and they serve to identify how, when, and where the indicator occurs and what part it plays in the overall scheme of operations.

b. Associations. Association is the relationship of an indicator to other information or activities. Intelligence analysts compare their current observations with what has been seen in the past to identify possible relationships.

(1) Using the previous example, the enemy analyst knows that the GSE is used for fixed-wing transport aircraft. The analyst also knows that the length and composition of the landing strip will only support transport aircraft as large as a C-130. Additionally, U.S. Marine forces are the only units that have used this field in the last two years. An analyst would likely take the GSE indicator and associate it with the previous information, and conclude that KC-130s are operating in the area.

(2) Another aspect to associations involves the continuity of actions, objects, or other indicators that register as patterns to an analyst. These indicators may not be the result of planned procedures, but may result from repetitive practices or sequencing to accomplish a goal. Using the earlier example, two more GSE units are observed at the same airbase. Past repetitive practices observed indicated that three GSE units signify a detachment of six KC-130s conducting operations in the area.

(3) Another useful association involves organizational patterns. Most military forces have a symmetrical organization. For example, an infantry headquarters company observed in the area

signifies an entire infantry battalion in the area. Thus in many situations, a pattern taken as a whole can be derived from a single indicator.

c. Profiles. Each functional activity generates its own set of unique signatures and associations. The sum of these signatures and associations is the activities profile.

(1) Given sufficient data, an analyst can determine the profile of any activity or unit. Over time, analysts attempt to identify and record the profiles of their adversary's activities or units. For example, an infantry regiment has many unique indicators. Over a period of several years, the enemy analysts have cataloged these indicators and created a standard picture, or profile of the indicators an infantry regiment creates. The enemy observes many indicators, compares them to their database, and can identify what type of unit is there.

(2) A profile for a major organization has subprofiles for functional activities needed to effect the operation. Observation of one or several of these subprofiles can be associated with the major profile to accurately predict what type of operation will occur. For example, the enemy observes indicators, compares them to their database, and then can identify what type of unit is there. If they had identified the profiles for a heavy weapons company and an infantry battalion, they will probably conclude that there is a regimental-size unit conducting operations.

d. Contrasts. Contrasts are differences observed between an activity's standard profile and current or recent activities.

(1) The deviation from the established profile is relatively easy to detect and will attract the enemy analysts attention. The analyst will then focus more intelligence collection efforts to find out what the "contrast" signifies. For example, the enemy identifies a profile of what appears to be an infantry unit, but observes indicators that do not fit that standard profile. The enemy then focuses it's collection efforts and observes more indicators. Comparing these indicators to the "profiles" database reveals that there are units there that fit the "profile" for a Marine Expeditionary Unit (MEU) force.

e. Exposure. Exposure refers to when and for how long an indicator is observed. The duration, repetition, and timing of an indicators exposure can affect its relative importance and meaning. Limiting the exposure period reduces the amount of detail that can be observed and the associations that can be formed.

(1) An indicator that appears over a long period of time will be assimilated into an overall profile and assigned meaning. An indicator that appears periodically will be further studied as a contrast to the normal profile. More detail can be gleaned from each exposure, adding to its meaning and relationship to a profile.

(2) An indicator that appears only briefly, and then disappears, may arouse strong interest or little, depending on the detail observed and value assigned. Limiting an indicators exposure in

time and occurrence will make it hard for the enemy to detect and evaluate the indicator.

(3) For example, using good OPSEC measures during the MEU workup exercises will limit the contrasts observed from the normally observed infantry battalion profile. This can shield the composition of the force, and prevent the enemy analysts from knowing that it is a MEU-level operation. This can further confuse the enemy to the purpose of the operation.

2. Examples of Indicators.

a. Indicators of General Military Capabilities:

(1) The presence of unusual types of units for a given area or base.

(2) Friendly reactions to adversary exercises or actual hostile actions.

(3) Actions, information, or material associating reserve units with specific commands or units (e.g., T/O for mobilization).

(4) Actions, information, or material indicating the levels of manning, readiness, and experience of personnel and/or units.

(5) Actions, information, or material revealing spare parts availability for equipment or systems.

(6) Actions, information, or material indicating equipment or systems reliability (e.g. visits of technical representatives or special repair team/unit).

(7) Movement of friendly ships, aircraft, and/or ground units in response to detection of enemy activities.

(8) Actions, information, or material revealing tactics, techniques, and procedures employed in different types of training exercises or during equipment/systems operational tests and evaluation.

(9) Stereotyped patterns in performing the organizational mission that reveal the sequence of specific actions or when and how they are accomplished.

b. Indicators of General Command and Control Capabilities.

(1) Actions, information, or material providing insight into the volume of orders and reports needed to accomplish a specific task or operation.

(2) Actions, information, or material showing unit subordination for deployment, mission, or a task.

(3) Association of particular commanders with patterns of behavior in various tactical situations.

(4) Information revealing problems of coordination between the commander’s staff elements or subordinate units.

(5) In exercises or operations, indications of the period between the occurrence of a need to act or react and the action taking place; of consultations that occur with higher commands, and the types of actions initiated afterward.

(6) Unusual actions with no apparent direction reflected in communications.

c. Indicators from Communications.

(1) Personnel using handheld radios; or testing aircraft, vehicle, or man-packed radios.

(2) Establishing and testing new communication nets. Without conditioning the enemy, the sudden appearance of a new net may cause the enemy to increase intelligence collection efforts.

(3) Increasing, decreasing, or ceasing (radio silence) radio transmission when close to starting an operation, exercise, or test. Again, without conditioning the enemy, unusual changes will catch the enemy’s attention.

(4) Using the same or common call signs for units, certain individuals (e.g., for the commander “6”); code words for activities, or conditions (e.g., “Winchester”); or infrequently changing radio frequencies and encryption. This allows for easier enemy monitoring and adds to “profiles.”

(5) Using stereotyped message characteristics that indicate particular types of activity allowing adversary’s to monitor and evaluate friendly activity.

(6) Requiring check-in and check-out with multiple or consistent control stations before, during, and after an activity (e.g., air operations).

d. Indicators for Equipment and Systems.

(1) Unencrypted emissions during tests and exercises.

(2) Budget data that provide insight into the objectives and scope of system research and development effort or sustainability of a fielded system (this often comes from public media).

(3) The equipment or system hardware itself.

(4) Information on test and exercise schedules that allow adversaries to better plan the use of intelligence collection efforts.

(5) Deployment of unique units, targets, and sensor systems to support tests associated with particular equipment or systems.

(6) Unusual visible security imposed on particular development effort that highlights their significance.

(7) Information indicating special manning for tests or assembly of personnel with special skills from manufacturers known to be working on a particular contract or activity.

(8) Notices to Airmen and Mariners (NOTAMS) that might highlight test areas and a particular operation.

(9) Stereotyped use of location, procedures, and sequences of actions when preparing for and executing test activities for specific types of equipment or systems.

(10) Use of advertisements that a company has a contract on a system, or possesses military technology.

e. Indicators of preparations for Operations. Many indicators deal with the preparatory phase, as opposed to the execution phase. Much of this is logistical in nature.

(1) Provisioning of special supplies.

(2) Requisitioning of special or an unusual volume of supplies to be filled by a particular date.

(3) Embarking special units, installing special capabilities, and preparing unit equipment with special configurations (e.g., desert paint schemes).

(4) Increased prepositioning of ammunition, fuel, weapons, and other types of supply items.

(5) Procuring large numbers or unusual types of maps/charts for a particular area.

(6) Making medical arrangements, mobilizing medical personnel, stockpiling pharmaceuticals (e.g., anthrax vaccine) and blood stocks.

(7) Focusing intelligence and reconnaissance assets on a particular geographical area or type of activity.

(8) Requisitioning or assigning an increased number of linguists of a particular language or related group of languages to an area.

(9) Initiating and maintaining unusual liaison with foreign nationals or governments for political or military support.

(10) Providing increased or specific types of training to personnel.

(11) Holding rehearsals to test aspects of an operation.

(12) Increasing the number of trips and conferences for senior officials and staff members.

(13) NOTAMS making seaport and airspace reservations/restrictions.

(14) Arranging for tugboats and pilots at seaports; requesting supplies or provisions for support at seaports.

(15) Recalling personnel on leave and liberty to their duty locations; canceling leave and liberty.

(16) Imposing unusual off-limits restrictions.

(17) Preparing units for combat operations through equipment checks as well as operational or maintenance stand downs in order to achieve a required readiness level for equipment and personnel.

(18) Making billeting and transportation arrangements for particular units or personnel.

(19) Taking large-scale action to change mailing addresses or arrange for mail forwarding; providing for wills and powers of attorney.

(20) Posting supply delivery, personnel arrival, transportation, or ordnance loading schedules in a manner where people without a need to know have access.

(21) Storing boxes, equipment, or other supplies in an uncontrolled area with labels or shipping forms indicating the destination or the operation name.

(22) Employing uncleared personnel to handle material used only in particular types of operations or activities.

(23) Providing unique or highly visible physical security arrangements for loading or guarding special munitions or equipment.

(24) Requesting unusual or increased meteorological, oceanographic, or ice information for a specific area/region.

(25) Setting up wide area network (WAN) over commercial lines.

f. Indicators during the execution phase.

(1) Unit and equipment departures from base.

(2) Enemy radar, sonar, or visual detection of friendly units.

(3) Friendly unit identifications through improper communications or physical observation of unit symbols (e.g. placards with unit ID, squadron ID on aircraft).

(4) Force composition and tracks or routes of advance that can be provided by emissions from units or equipment and systems that provide identifying data.

(5) Stereotyped procedures; static and standard ways of composing, disposing, and controlling strike and defensive elements against particular threats; and predictable reactions to enemy reactions or operations.

(6) Trash and garbage dumped by units or from ships at sea, or picked up by commercial vendors that might provide identifying data or other information.

(7) Alert of civilians in operational areas.

(8) Transportation or requisitioning of spare parts or personnel to deploying or deployed units via military or commercial means.

(9) Changes in oceanographic high frequency transmission.

(10) Changes in activity, volume over the WAN.

g. Indicators of Post engagement operations or Residual Capabilities.

(1) Repair and maintenance facility schedules.

(2) Urgent, increased, or unusual requests for maintenance personnel, units, equipment, or supplies.

(3) Movement of supporting maintenance resources.

(4) Unusual medical activity.

(5) Unusual re-supply of a unit or activity.

(6) Assignment of new units to an area.

(7) Search and rescue activity.

(8) Personnel orders or reassignment.

(9) Discussion of repair, maintenance, or supply issues in unsecure areas or by unsecure means.

(10) Termination or modification of procedures for reporting of unclassified meteorological, oceanographic, or ice information.

EXAMPLES OF CRITICAL INFORMATION

1. Diplomatic Negotiations.

a. Military capabilities and intentions (pre-treaty and post-treaty).

b. Minimum negotiating positions.

c. Intelligence verification and collection capabilities.

2. Political and Military Crisis Management.

a. Target selection and deployment destinations.

b. Timing considerations.

c. Logistical capabilities and limitations.

d. Alert posture, Defense Condition, and response time.

3. Mobilization.

a. Intent to mobilize before public announcement.

b. Impact on military industrial base.

c. Impact on civilian economy.

d. Transportation capabilities and limitations.

4. Military intervention.

a. Intentions.

b. Military capabilities.

c. Strategy and tactics.

d. Forces assigned and in reserve.

e. Targets.

f. Time considerations.

g. Routes for combat units, support units, and resupply.

h. Logistic capabilities and constraints.

i. Third-nation or host-nation arrangements.

5. Open Hostilities.

a. Force composition, disposition.

b. Attrition and reinforcement.

c. Targets.

d. Time considerations.

e. Logistic capabilities and constraint.

f. Location of C2W asset.

6. Intelligence, Reconnaissance, and Surveillance.

a. Purpose of collection efforts.

b. Targets of collection.

c. Time considerations.

d. Types of and capabilities of collection assets.

e. Processing capabilities.

f. Units requesting intelligence data.

7. Peacetime Weapons and other Military Movements.

a. Fact of movement.

b. Origin and destination of units, personnel, and equipment being moved.

c. Capabilities of units, personnel, and equipment being moved.

d. Inventory of equipment being moved.

8. Command Post and Field Training Exercises.

a. Participating units.

b. OPLAN or other contingencies that are being exercised.

c. Command relationships.

d. Command, control, communications, and computer connections and weaknesses.

e. Logistics capabilities and weaknesses.

9. Noncombatant Evacuation Operations.

a. Targets.

b. Forces involved.

c. Logistic capabilities and constraints.

d. Safe havens or staging areas.

e. Routes.

f. Time considerations.

10. Counterdrug Operations.

a. Military forces involved.

b. Law enforcement agencies (LEAs) involved.

c. Military support to LEAs.

d. Host-Nation cooperation or involvement.

e. Capabilities of military forces/LEAs.

f. Time considerations.

g. Tactics to be used.

h. Logistic capabilities and constraints.

11. Counterterrorism Operations.

a. Forces.

b. Contingency plans.

c. Standing SOP.

d. Targets.

e. Time considerations.

f. Staging or basing locations.

g. Tactics.

h. Ingress and egress methods.

i. Logistic capabilities and constraints.

EXAMPLES OF OPSEC MEASURES

1. Operational and Logistic Measures.

a. Randomize the performance of functions and operational missions. Avoid repetitive or stereotyped tactics and procedures for executing operations and activities in terms of time, place, event, sequencing, formations, and command and control arrangements.

b. Employ force dispositions and command and control arrangements that conceal the location, identify, and command relationships of major or important units.

c. Conduct support activities in a way that will not reveal intensification of preparations before initiating operations.

d. Transport supplies and personnel to combat units in such a way to conceal the location and identity of combat units.

e. Operate aircraft at a low altitude to avoid detection.

f. Operate and deploy units or weapons systems in a way to minimize the reflective surfaces exposed to radar and sonar.

g. Use darkness to mask deployments or force buildup.

2. Technical Measures.

a. Use proper radio procedures and techniques to minimize interception and evaluation of emissions. Use techniques such as burst transmissions, secure phones, couriers, encrypted transmission, and frequently changing codes and encryptions. Limit use of high frequency radios and directional super-high frequency transponders.

b. Control radar emissions, operate at reduced power, and operate radars common to many units.

c. Mask emissions, forces, and equipment from radar or visual detection by use of terrain.

d. Use appropriate IO deception or jamming. Use camouflage, smoke, background noise, or inclement weather to conceal movement of personnel, units, and equipment (be aware that this might create a contrast and attract the enemy’s attention without conditioning or integration into a deception package).

3. Administrative Measures.

a. Avoid bulletin board notices, plan of the day, or planning schedule notices that reveal when events will occur (or other specific details).

b. Conceal budgetary transactions, supply request and actions, and arrangements for services that reveal preparations or intentions for operations.

c. Conceal the issuance of orders, the movement of special personnel and/or equipment to units, and the addition of special capabilities to units.

d. Control trash disposal and other housekeeping functions to conceal the identity and location of units, and other details pertaining to the operation.

e. Follow normal leave and liberty policies to the maximum extent possible to present a sense of normalcy.

f. Ensure that personnel discretely prepare for their family’s welfare in their absence.

4. Military Deception in support of OPSEC. Use to:

a. Cause enemy intelligence to not target friendly activities, ensuring failure to collect intelligence against our tests, operations, and exercises. To prevent the enemy from determining through analysis vital capabilities and characteristics of weapon, systems, and vital aspects of policy, doctrine, and tactics.

b. Create confusion about, or cause multiple interpretations of intentions, operations, tactics to be employed, and timetables.

c. Create confusion about or cause multiple interpretations of vital information taken from open sources.

d. Cause enemy observers to lose interest in the test, operation, exercise, or activity; or to assign a low priority to intelligence collection efforts.

e. Convey inaccurate locating and targeting information to the enemy.

5. Physical destruction and Electronic Warfare. During hostilities, use physical destruction and electronic attack against the enemy’s assets used to collect and process intelligence. Offensive IO actions that can be conducted include: strikes against satellites; communications centers or sites; radars; fixed sonar sites; reconnaissance aircraft, ships, or units.

THE OPSEC PROCESS

The OPSEC Process involves five steps applied in a sequential order. In dynamic situations, the steps may be revisited at any time to adjust to new threats or information.

1. Step 1: Identification of Critical Information. The commander and staff tries to identify the questions that they believe the enemy will need to know about friendly intentions, capabilities (and limitations), and activities. These questions are the essential elements of friendly information (EEFI). Critical information is only part of the EEFI, it is the information vitally needed by the enemy. This serves to focus the OPSEC Process on protecting the vital information, rather than attempting to protect all information. The EEFI is found in the OPLAN in Tab C to Appendix 3 to Annex C (Operations). This critical information will often times be similar to what you would want to know about the enemy.

2. Step 2: Analysis of Threats. This involves the research and analysis of intelligence information, counterintelligence, reports, and open source information to identify whom the likely enemy will be. The friendly commander will ask questions, such as:

a. Who is the enemy or adversary? Who has intent and capability to take action against us?

b. What are the enemy's intentions and goals?

c. What is the enemy's strategy for opposing the planned operation? What type of tactics and forces will the enemy employ?

d. What critical information does the enemy already know about the operation or friendly forces? What critical information is it too late to protect? Are their OPSEC measures that can be taken later in the process to protect critical information or deceive the enemy on compromised critical information?

e. What are the enemy's intelligence collection capabilities? How does the enemy process and disseminate their collected data? Friendly intelligence and counterintelligence staffs can provide this.

3. Step 3: Analysis of Vulnerabilities. This action identifies an operation's or activity's vulnerabilities. This requires examining the parts of the planned operation and identifying OPSEC indicators that could reveal critical information. Vulnerabilities exist when the enemy is capable (with the available collection and processing assets) of observing an OPSEC indicator, correctly analyzing it, and then taking appropriate and timely action. Reviewing results of preparations (workups) to the operation such as computer simulations, war games, sand table exercises, field exercises, and command post exercises will help identify vulnerabilities not readily apparent. The commander will need answers to questions such as these:

a. What OPSEC indicators of critical information not known to the enemy will be created by friendly actions that result from the planned operation or activity?

b. What OPSEC indicators can the enemy actually collect?

c. What OPSEC indicators can the enemy actually use to our disadvantage?

4. Step 4: Assessment of Risk. This step essentially has two components. First, planners analyze the identified vulnerabilities and then identify possible OPSEC measures against them. Second, specific OPSEC measures are selected for execution based on the risk assessment done by the commander and staff.

a. OPSEC Measures can be used to:

(1) Prevent the enemy from detecting an OPSEC indicator.

(2) Provide an alternate analysis of an indicator from the enemy viewpoint (deception).

(3) Directly attack the enemy's collection system(s).

b. Besides physical destruction, OPSEC measures can include:

(1) Concealment and camouflage.

(2) Deception (across all aspects of operations and IO).

(3) Intentional deviations from normal patterns; and conversely, providing a sense of normality.

(4) Practicing sound information security, physical security, and personnel security.

c. More than one OPSEC measure may be identified for each vulnerability; and one OPSEC measure can be identified for multiple vulnerabilities. Primary and secondary OPSEC measures can be identified for single or multiple OPSEC indicators. OPSEC measures are most effective when they provide the maximum protection while minimally effecting operational effectiveness.

d. Risk assessment involves comparing the estimated cost (time, effort, resource allocation, and money) of implementing an OPSEC measure to the potential effects on mission accomplishment resulting from an enemy exploiting a particular vulnerability. Questions to ask include:

(1) What is the risk to mission effectiveness if an OPSEC measure is taken?

(2) What is the risk to mission effectiveness if an OPSEC measure is not taken?

(3) What is the risk to mission effectiveness if an OPSEC measure fails to be effective?

(4) Will the cost of implementing an OPSEC measure be too much as compared to the enemy's exploitation of the vulnerability?

(5) Will implementing a particular OPSEC measure create an OPSEC indicator? Will it create an OPSEC indicator that you want the enemy to see (e.g., deception)?

(6) Do we even have the capability to implement the OPSEC measure? If we do, can the assets under our control accomplish this, or do we need to request assets from outside sources?

e. Planning for OPSEC measures requires coordination amongst all staff elements, and supporting elements or assets outside the command. Particular care must be taken to ensure that OPSEC measures do not interfere with other operations (e.g., deception plans, psychological operations). Solid staff functioning and planning will ensure OPSEC plans integrate with and support other programs and operations.

5. Step 5: Application of OPSEC Measures. In this step, the commander implements the OPSEC measures selected in the previous step (Risk Assessment). Planning and integrating OPSEC measures into the OPLAN is critical to ensure counter measures are applied at the right time, place, and manner.

a. The enemy reaction to our OPSEC measures will be monitored to determine effectiveness. Provisions and methods for feedback from combat units, intelligence and counterintelligence staffs, and other IO elements, will have to be planned for in the OPLAN. This feedback will help determine the following:

(1) Is the OPSEC measure producing the desired effect? Or is it producing an undesired effect?

(2) Is the OPSEC measure producing an unforeseen effect? If so, does this result in positive or negative effects for friendly forces?

(3) Do we need to continue executing the OPSEC measure? Will it still be effective, or has it accomplished its task and been overcome by the tempo of operations?

(4) Do we need to cease the OPSEC measure because of no observable results, negative, or unintended consequences?

(5) Do we need to modify the OPSEC measure based on the result?

(6) Do we need to implement previously selected (secondary) OPSEC measures to replace ineffective OPSEC measures based on the results?

(7) Do we need to devise new OPSEC measures to replace ineffective OPSEC measures?

(8) Have we identified new requirements, or unforeseen OPSEC indicators that will need new OPSEC measures? Again, this is dynamic process, and previous steps may have to be revisited.

b. In addition to ongoing operations, feedback provides information for OPSEC planning for future operations through “lessons learned.”

c. The OPSEC Survey is an excellent method and tool for providing feedback on the effectiveness of OPSEC measures.

THE OPSEC SURVEY

1. The purpose of the OPSEC Survey is to determine if adequate protection from enemy intelligence collection exist. The survey will determine if critical information is being protected during an operation or activity. Critical information has to have been identified during the OPSEC Process for this to happen.

2. Each OPSEC survey is unique because of the different activities of varying units within the Marine Corps. Additional factors are the nature of the information to be protected, the enemy's intelligence collection capabilities, and the environment of the activity to be surveyed.

3. OPSEC surveys differ from security inspections in that security inspections seek to ensure compliance with directives and regulations concerning classified or unclassified material, and security of physical structures/installations. However, survey teams should also ensure that security measures are not creating OPSEC indicators.

4. Surveys are not to be used as a punitive tool, but should be conducted on a non-attribution basis. This will ensure better cooperation and honesty when surveying activities, plans, and operations.

5. Results of surveys should be given to the commander of the unit surveyed. Results may also be forwarded to higher headquarters on a non-attribution basis to derive lessons learned that may be applied to other units within the Marine Corps.

6. OPSEC surveys can be accomplished by either a command or formal survey. A command survey is conducted by members within the command for that command and attached units. A formal survey is composed and conducted by members from within and outside the command. The formal survey will often cross command lines, and needs to be coordinated appropriately. Formal surveys are normally directed by higher headquarters to subordinate echelons, but may be requested by subordinate commands.

7. The OPSEC Survey is composed of the following phases (planning, field survey, and analysis and reporting):

a. OPESEC Survey Planning Phase.

(1) Determine the Scope of the Survey. Limit the extent of the survey to manageable proportions based on time, geography, units to be observed, operations or activities to be observed, staffing, funding, and other practical considerations.

(2) Select the Survey Team Members. Select members from the various staff functions (e.g. intel, comm, logistics, admin, ops) and other entities as needed (e.g. public affairs) to ensure an adequate breadth of expertise. OPSEC is an operations function, so the team OIC should be from the S-3/G-3.

(3) Understand the Operation or Activity to be Surveyed. Team members must be thoroughly briefed on the operation plan, and any other

matters affecting the operation. This will help team members develop a functional outline for the aspect of the operation they are responsible to survey.

(4) Determine the Enemy's Intelligence Collection capabilities. Intelligence and counterintelligence staffs will normally provide this information (found in annex B of the OPLAN).

(5) Conduct Empirical Studies (if possible). An example would be to review results of preparations (workups) to the major operation; such as, computer simulations, war games, sand table exercises, field exercises, and command post exercises. This may already be available from information used to complete step 3 of the OPSEC Process. These reviews can help the team identify vulnerabilities that cannot be determined through observation of the operation and interviews of personnel.

(6) Develop a Functional Outline. Functional outlines for each functional area to be surveyed will be completed.

(a) Start by developing a timetable of events to occur. Comparing the event chronology with the known or projected enemy intelligence collection capabilities can often identify vulnerabilities not previously identified. All of the functional chronologies can later be correlated to build the big picture of the operation.

(b) Next, use the chronology to build a functional outline. An example is provided on the next page. The functional outlines project a time-phased picture of events associated with the planning, preparation, execution, and conclusion of the operation. The outline provides an analytical basis for identifying events and activities that are vulnerable to enemy exploitation.

(7) Determine the Vulnerabilities. Review of the OPSEC Plan in the OPLAN, the projected enemy intelligence threat, the chronology of events, and any empirical studies will identify the potential OPSEC indicators. Friendly vulnerabilities can now be confirmed or identified.

(8) Determine Procedures to Conduct the Survey. Develop any SOP needed, including coordinating for free access to units and personnel. Determine if any training is required, or if members need familiarization with a particular functional area (if they do not have expertise in that area).

(9) Announce the Survey. Announce the survey far enough in advance to allow the command to prepare for the survey, and to support the survey team. Include in the announcement:

(a) Survey purpose and scope.

(b) List of team members and clearances.

(c) List of required briefing and orientations.

(d) Timeframe involved.

(e) Administrative or Logistical support requirements.

(f) Any other details deemed pertinent.

EXAMPLE OF A FUNCTIONAL OUTLINE

The outline below can be applied to all the different functional areas such as intelligence, logistics, communications, operations, and administration and support.

1. Planned Event Sequence. The OPLAN and command/staff briefs form the basis for this timeline. This can be formulated using a lineal listing, a matrix, or another suitable method as required.

2. Actual Event Sequence. Observe and record events as they actually occur while surveying activities. Be especially cognizant of the information listed in paragraphs three through five below.

3. Critical Information. List critical information that the command has identified in their OPLAN (annex B).

4. OPSEC Indicators. List OPSEC indicators of critical information that you expect to see based on review of the OPLAN (annex B) and command/staff briefs prior to field survey commencing.

5. OPSEC Measures. List the OPSEC measures developed in the OPLAN (annex B) that you can expect to see during the survey.

6. Analysis. Determine any OPSEC vulnerabilities through review of OPLAN (annex B), command/staff briefs, and actual activities/operations observed. You are looking for OPSEC indicators that can reveal critical information. This condition creates a vulnerability that can be exploited by the enemy. Are the identified OPSEC measures effective in protecting the critical information by preventing the enemy from collecting and accurately interpreting the OPSEC indicators?

OPSEC FIELD SURVEY PHASE

1. This phase involves observing operations/activities, reviewing documents, and interviewing personnel. The following actions are required:

a. Conduct a Command Brief. This action is a two-step brief. The commander and staff brief the operation to the survey team. The survey team should take this opportunity to clarify questions developed in the planning phase; then the survey team briefs the command on the survey objectives and procedures. Include in the brief a summary of the hostile threat collection capabilities and the vulnerability assessment. The command should be asked to comment on this to validate the assessment. This brief to the command can be a formal presentation or informal discussion.

b. Refine the Functional Outlines. Using information from the command brief, make changes to the functional outlines as needed. During the actual survey, changes to the outline may also be needed as data is collected.

c. Collect the Data.

(1) Collect data using personnel interviews, document collection and review, and observations of activities in each functional area. Observe activities and operations using the functional outline as your guide.

(2) Survey members should assure the interviewees that the information they provide would be protected by a non-attribution policy. Interviews should cover the purpose of the interview; description and duties of the interviewee; details of the tasks performed as to exactly how, what, where, and when they perform them with a view toward determining what information they receive, handle, or generate, and what they do with it; whether the individual’s actions reflect an awareness of the hostile collection capabilities; and whether the interviewee’s actions produce OPSEC indicators.

(3) Incorporate the collected data into the functional outline. As the data is inputted, this changes the outline from a projection of events to a record of actual events. The outline then is a chronological record of what actually was done or happened, who did it, where it happened, and how and why it was done. The recordings should include an assessment of the identified vulnerabilities in light of the enemy collection threat, and any OPSEC indicators generated by the activities/operations.

(4) If a finding is considered to have serious negative mission impact, the commander should be notified to allow for early corrective action.

(5) Conduct a daily post brief among the survey team. This is a chance to compare and correlate data, assess the functional outlines and refine as needed, and redirect team efforts or members as needed.

ANALYSIS AND REPORTING PHASE

1. During this phase, the survey team correlates and assesses the data collected in the field survey phase.

2. Identify Vulnerabilities. Correlate and assess the data to identify vulnerabilities, those that were previously developed, and those that were identified during the field survey. OPSEC indicators that were observed are identified as potential vulnerabilities. Again, vulnerabilities are conditions that the enemy may be able to exploit to reveal critical information. The key characteristics of vulnerabilities are observable OPSEC indicators, and the enemy's ability to collect or observe the indicators. The ability of the enemy to be able to effectively exploit the vulnerability and in a timely manner indicates the actual risk to friendly forces.

3. OPSEC Survey Report. The report is generated, addressed, and delivered to the Commander of the operation/activity surveyed. A suggested format is included in this order. Format for findings can be presented in chronological order, order of significance, or grouped into the different functional areas. The report should discuss:

a. Observed OPSEC indicators.

b. Ability of the enemy to collect and process the indicators.

c. Vulnerabilities identified.

d. Analysis of the vulnerability's risk to the command's operations.

e. Recommended OPSEC measures or modification to existing OPSEC measures.

f. Answer the question, "Is the critical information being protected?"

g. Care must be taken to ensure the appropriate level of classification is given to discussions of vulnerabilities, and recommended OPSEC measures.

EXAMPLE FORMAT FOR FINAL OPSEC SURVEY REPORT

1. Overview.

a. Background. Address the purpose and scope of the OPSEC survey.

b. Conduct of Survey. Brief discussion of team composition, procedures used, units or commands visited, timeframes involved, and any problems encountered.

c. Critical information. List the critical information identified in the OPLAN.

d. Threat. List the enemy intelligence collection capabilities.

2. Findings, Analysis, Conclusions (Recommendations). This is the main body of this report. Discussions may be listed chronologically, by command, chronologically by commands, by the different functional areas, or a combination of all the above. Compress the recorded facts observed into the significant points. List the positive and negative points. The intent is to reinforce OPSEC that is working, and changing that which is not working or filling an existing void. The following is the suggested format for this section of the final report:

a. Observation. List the observed OPSEC indicators that could reveal identified information. This will include previously identified indicators (from the OPLAN and briefs); and indicators not previously identified but observed during the survey.

b. Analysis. Discuss the vulnerabilities observed. The key here is whether or not the enemy has the intelligence collection capability to observe and process the OPSEC indicators. If the command or other types of units (not involved in the operation) can reasonably expect to face future enemies that will have the collection capability, include this in the discussion. This information can be important to future operations and can be disseminated appropriately. The main points of your analysis will be whether or not the indicator revealed critical information. If so, then the OPSEC measure is not working. Did the OPSEC indicator even have an OPSEC measure applied to protect the critical information? If the OPSEC indicator revealed or can be inferred to have revealed critical information, then this condition is a vulnerability.

c. Recommendations. Recommend OPSEC measures to counter the OPSEC indicators, to protect the critical information. If the OPSEC Survey team does not have the expertise and knowledge to recommend an OPSEC measure, then be honest and state this. The command can then plan, develop, and apply appropriate OPSEC measures for future or current operations. The command needs to determine if OPSEC lessons-learned can be applied to other commands and disseminate the information appropriately. Care must be taken to appropriately classify and handle the final OPSEC Survey Report IAW the appropriate security directives.

INSPECTOR GENERAL'S 481 CHECKLIST

OPERATIONAL SECURITY

481H00H000H

Subcategory for MARFORLANT, MARFORPAC, and MARFORRES:

Function #	**Audit Statement**
481H00H001H	Does the command have a force level OPSEC order? Reference MCO 3432.1, paragraph 6.b.1
481H00H002H	Has the command designated in writing, those subordinate commands, activities, and installations that require an OPSEC program? Reference MCO 3432.1, paragraph 6.b.2
481H00H003H	Has the command delegated the authority in 481H00H002H to subordinate commanders in writing? Reference MCO 3432.1, paragraph 6.b.2
Subcategory for MCCDC, MCRC, and MATCOM:	
481H00H004H	Does the command have an OPSEC order? Reference MCO 3432.1, paragraph 6.c.1
481H00H005H	Has the command designated in writing, those subordinate commands, activities, and installations that require an OPSEC program? Reference MCO 3432.1, paragraph 6.c.2
Subcategory for Commanders requiring an OPSEC Program:	
481H00H006H	Does the command have an established OPSEC program? Reference MCO 3432.1, paragraph 6.d
481H00H007H	Has the command designated the responsible officer to develop, implement, and oversee the OPSEC program? Reference MCO 3432.1, paragraph 6.d.2
481H00H008H	Does the command have written commander's guidance and SOP for conducting a baseline OPSEC survey? Reference MCO 3432.1, paragraph 6.d.3, and enclosure (5)

481H00H009H Has a baseline OPSEC survey been conducted?
Reference
MCO 3432.1, paragraph 6.d.3, and enclosure (5)

481H00H0010H Is the command reviewing and updating the baseline OPSEC survey on an annual basis?
Reference
MCO 3432.1, paragraph 6.d.3

481H00H0011H Does the command have guidance and SOP for conducting OPSEC surveys for operations and activities as directed by the commander (note that this may be the same as guidance and SOP for 481H00H008H)?
Reference
MCO 3432.1, paragraph 6.d.4, and enclosure (5)

481H00H0012H Does the command have SOP for applying the OPSEC process to operational plans?
Reference
MCO 3432.1, paragraph 6.e.5, and enclosure (4)

481H00H0013H Is the command applying the OPSEC process to operations?
Reference
MCO 3432.1, paragraph 5.d, and enclosure (4)

481H00H0014H Does the command have SOP for annual review and update of the command's OPSEC program?
Reference
MCO 3432.1, paragraph 6.d.6

481H00H0015H Is the command conducting an annual review of the unit OPSEC program?
Reference
MCO 3432.1, paragraph 6.d.6

481H00H0016H Does the command OPSEC program provide for annual OPSEC training and awareness?
Reference
MCO 3432.1, paragraph 6.d.7

481H00H0017H Is the command conducting annual OPSEC training and awareness?
Reference
MCO 3432.1, paragraph 6.d.7

481H00H0018H Does the command coordinate with Public Affairs during the OPSEC planning process as needed for operations?
Reference
MCO 3432.1, paragraph 5.h